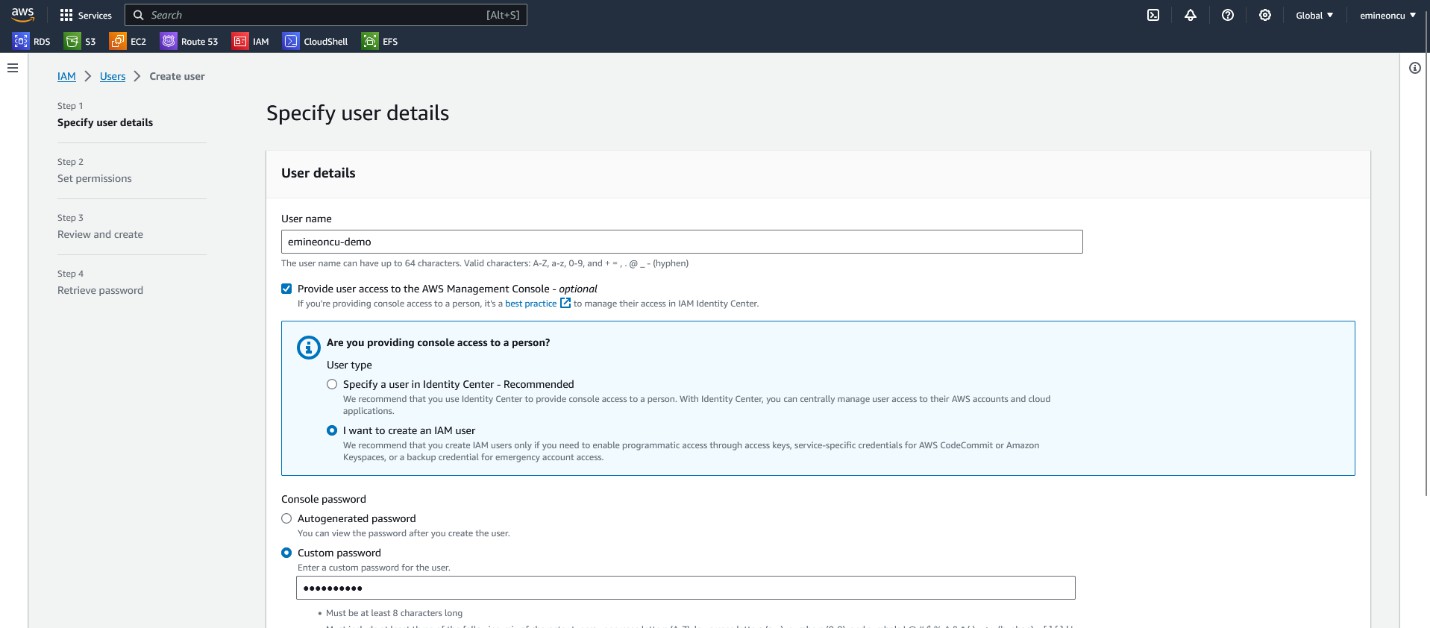
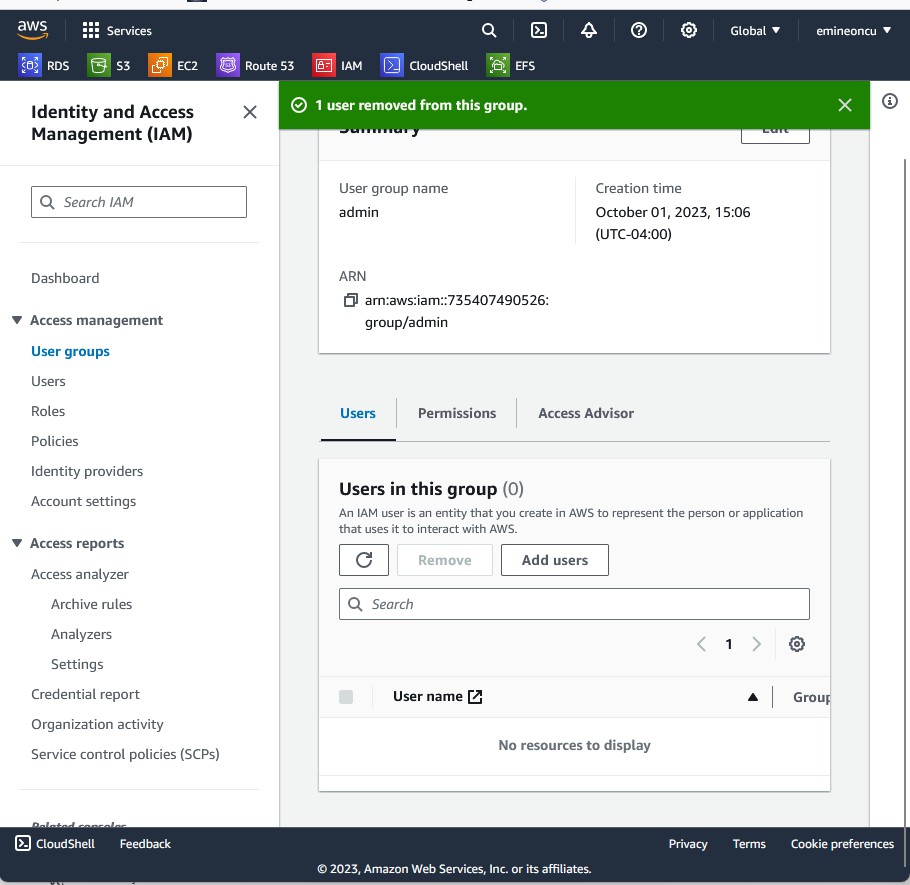
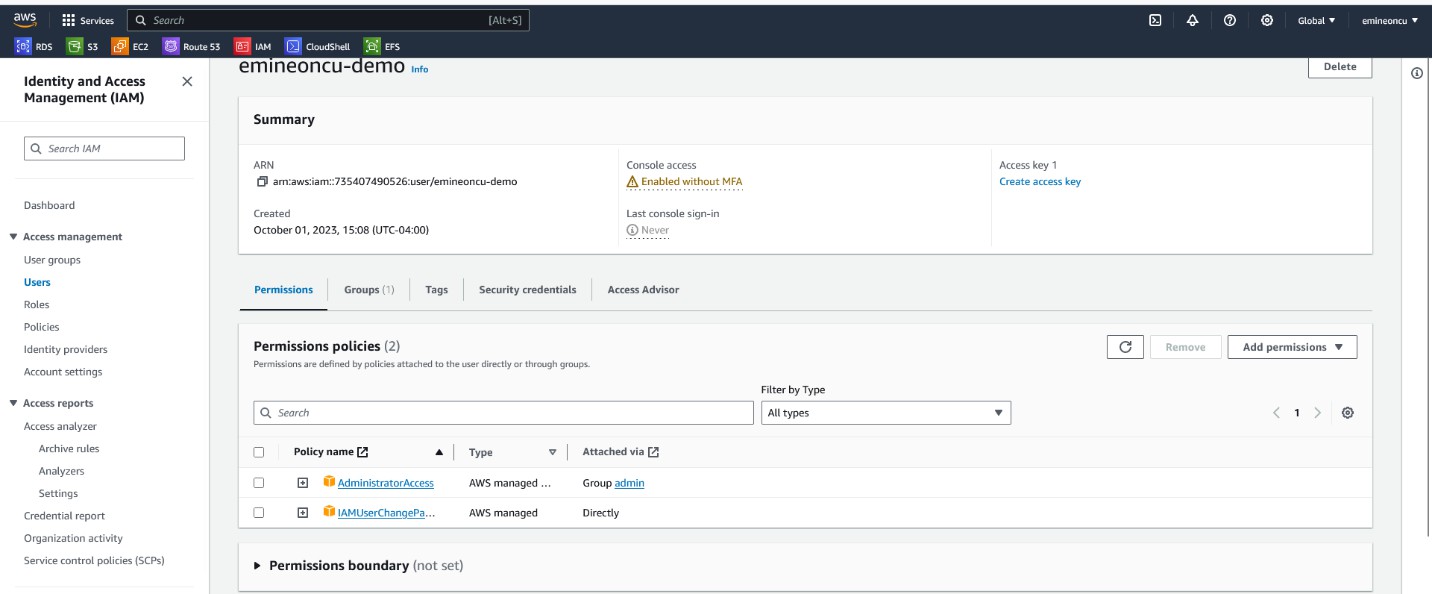
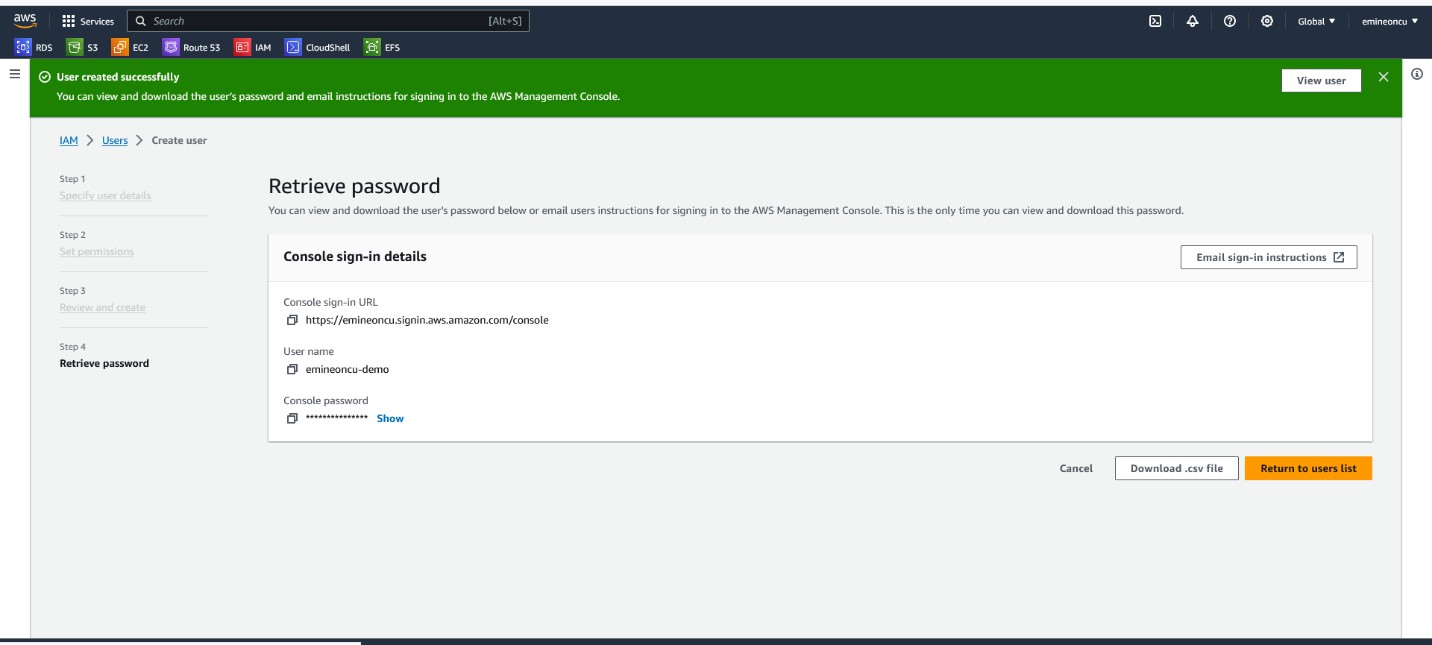
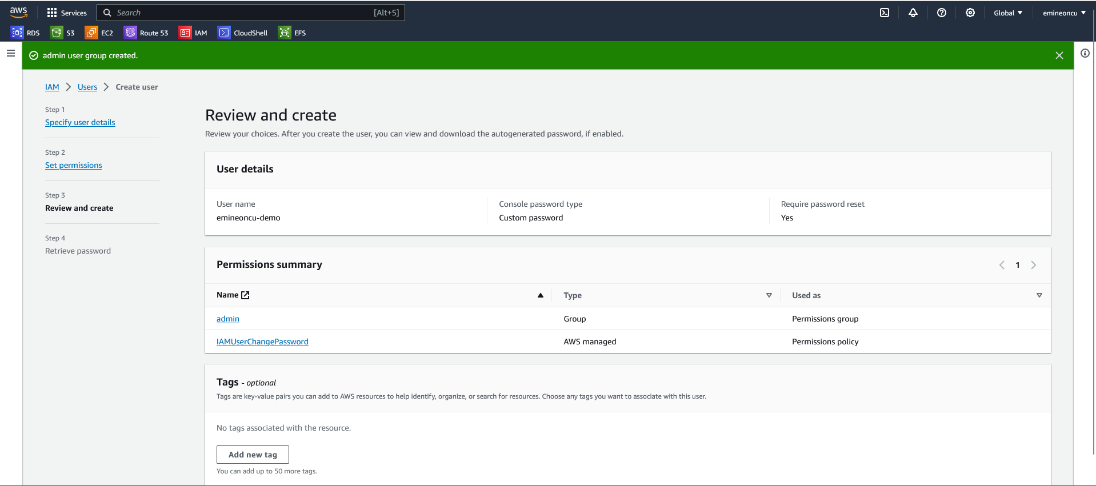
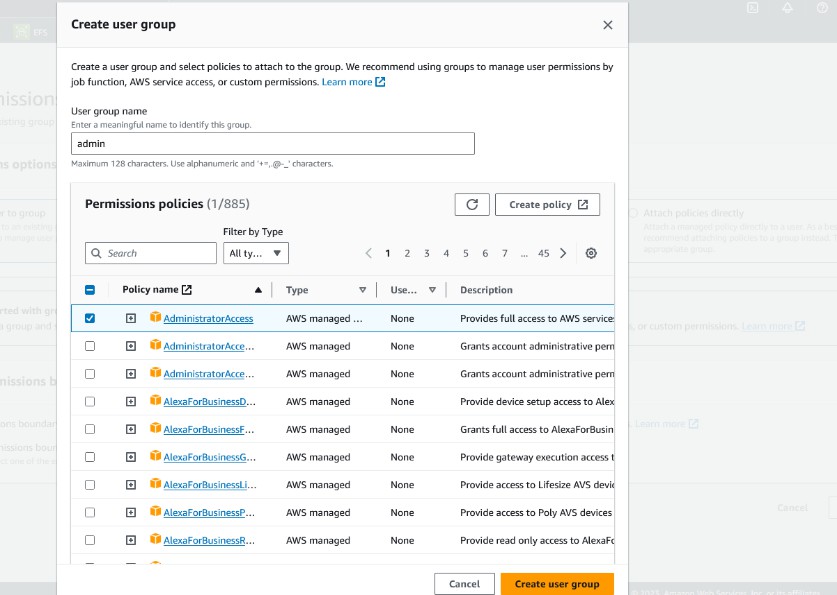
* **IAM is a Global Service, Creating a user with the name “emineoncu-demo”.**

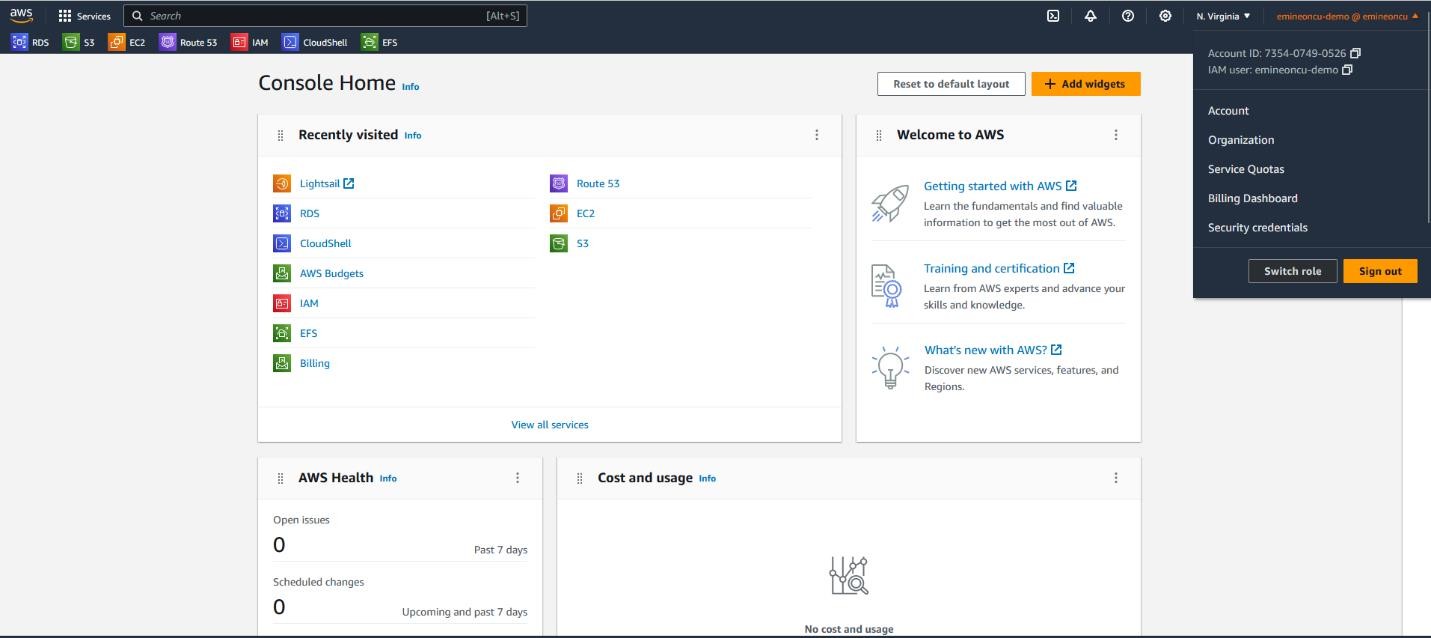


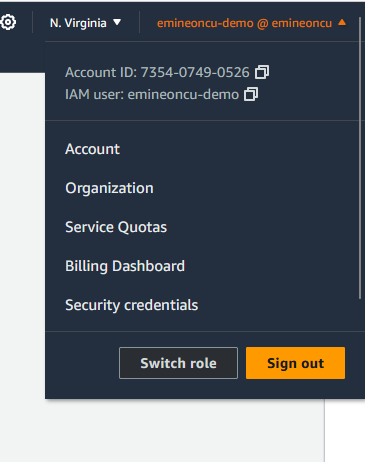
* **Creating a Group with the name admin and attach “Administrative Policy” to the group.**
* **Added the user to the group.**

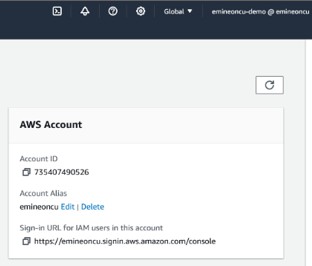


* ​

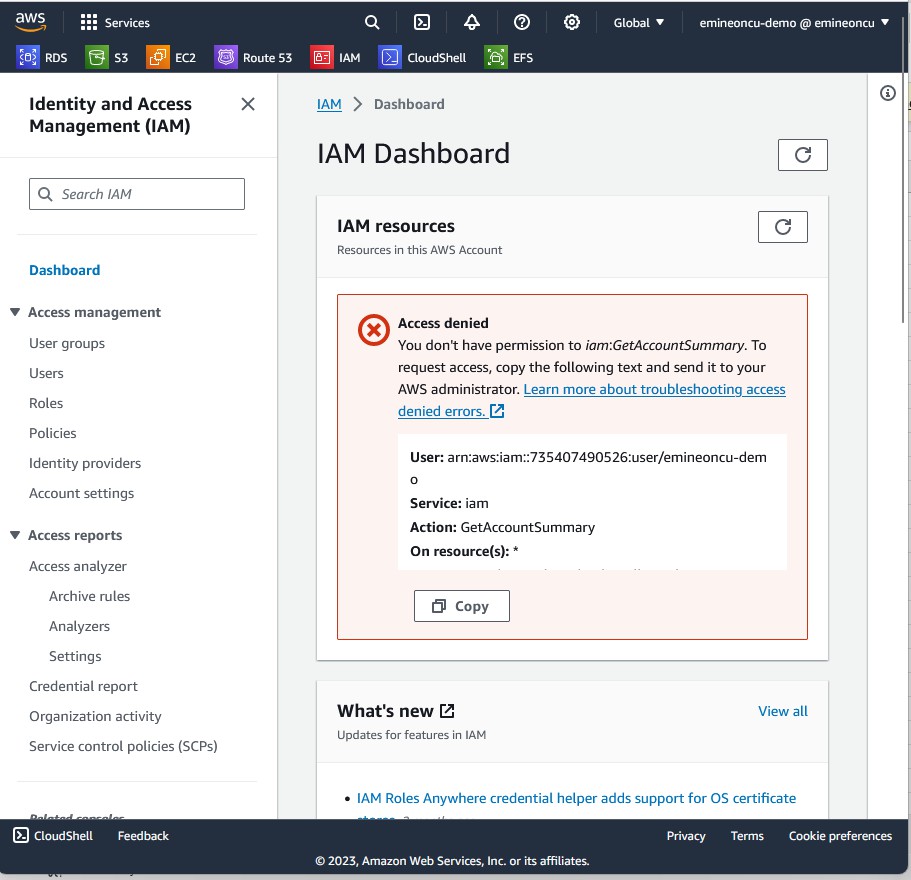
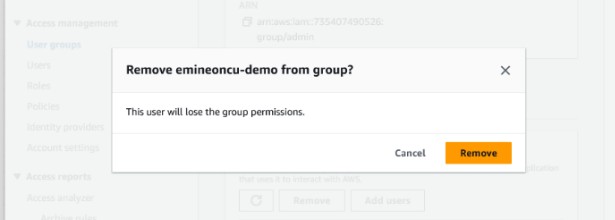




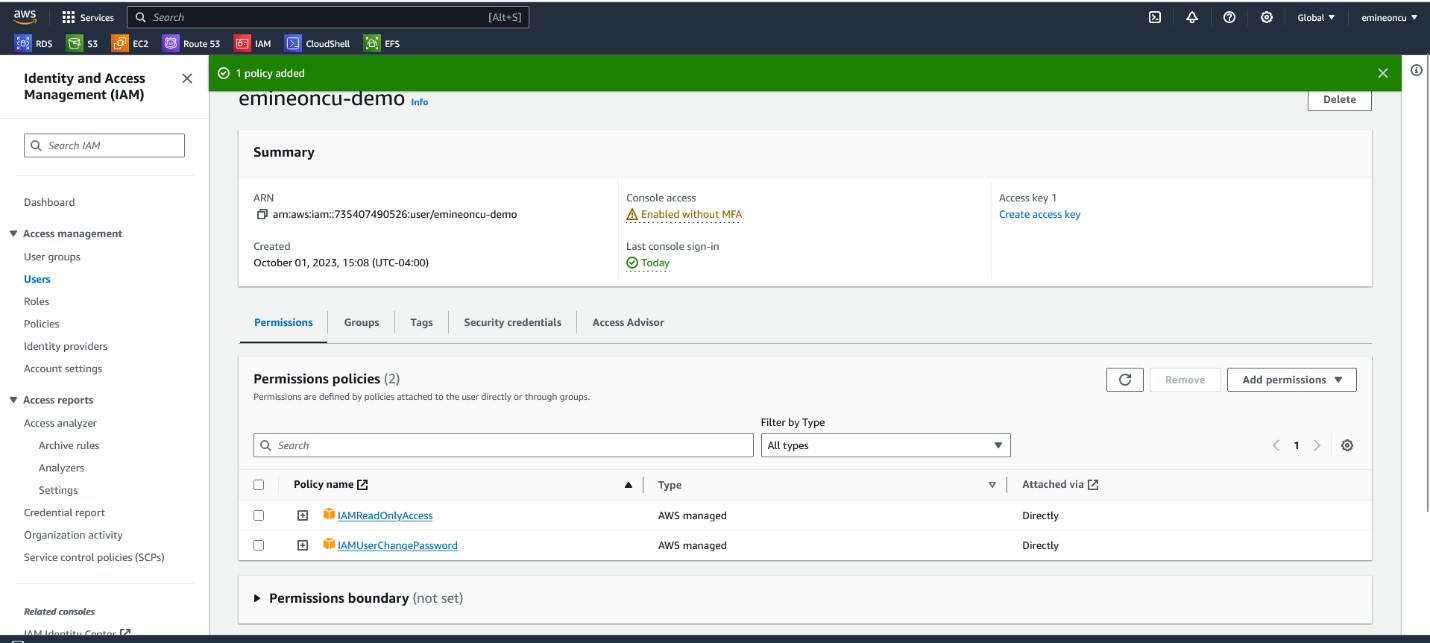
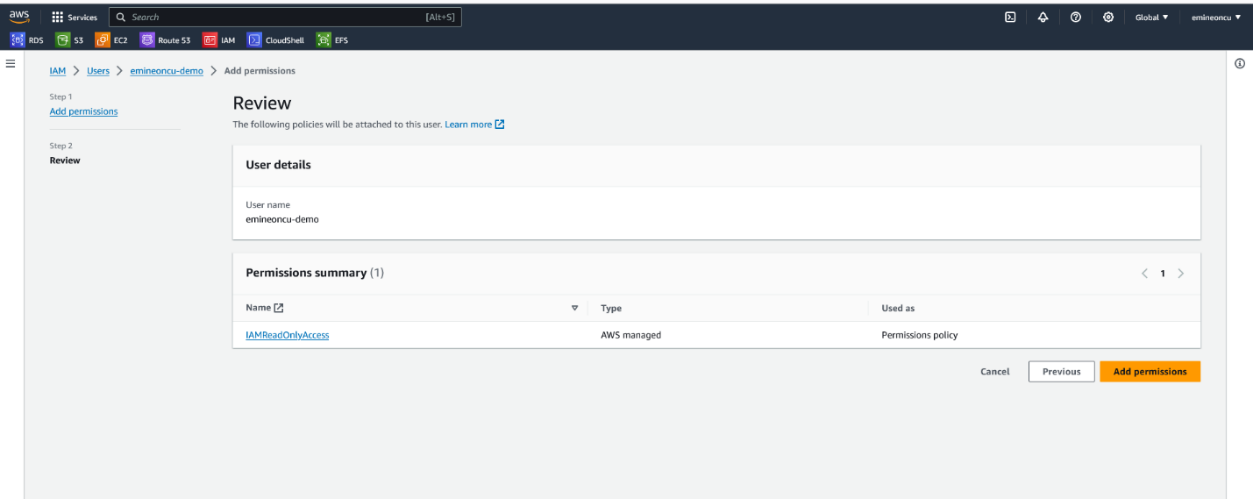
- Create an account alias so it is easier to remember while signing in



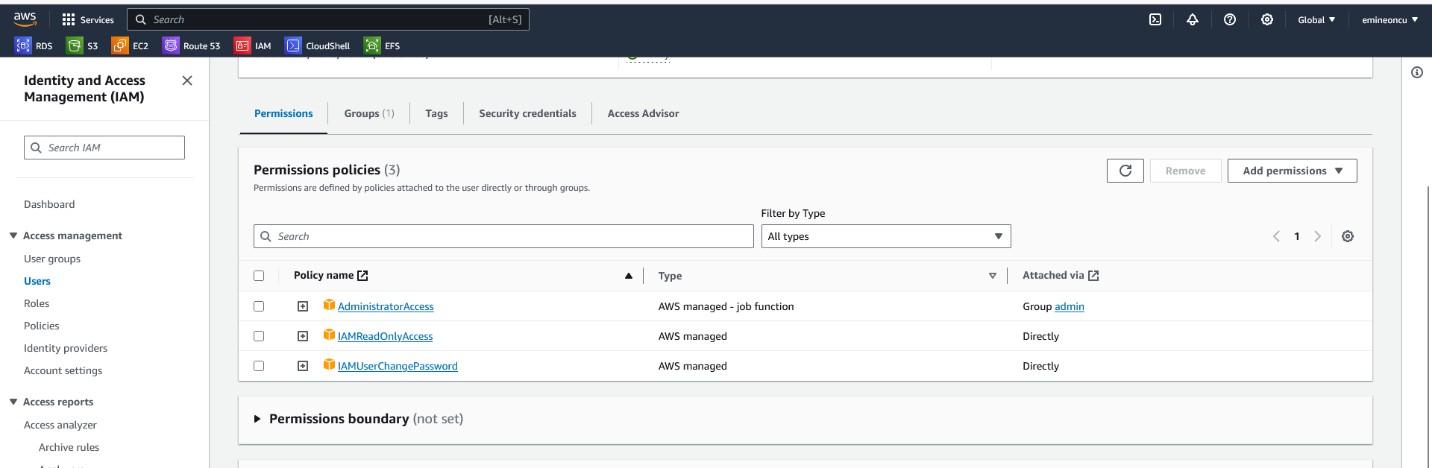
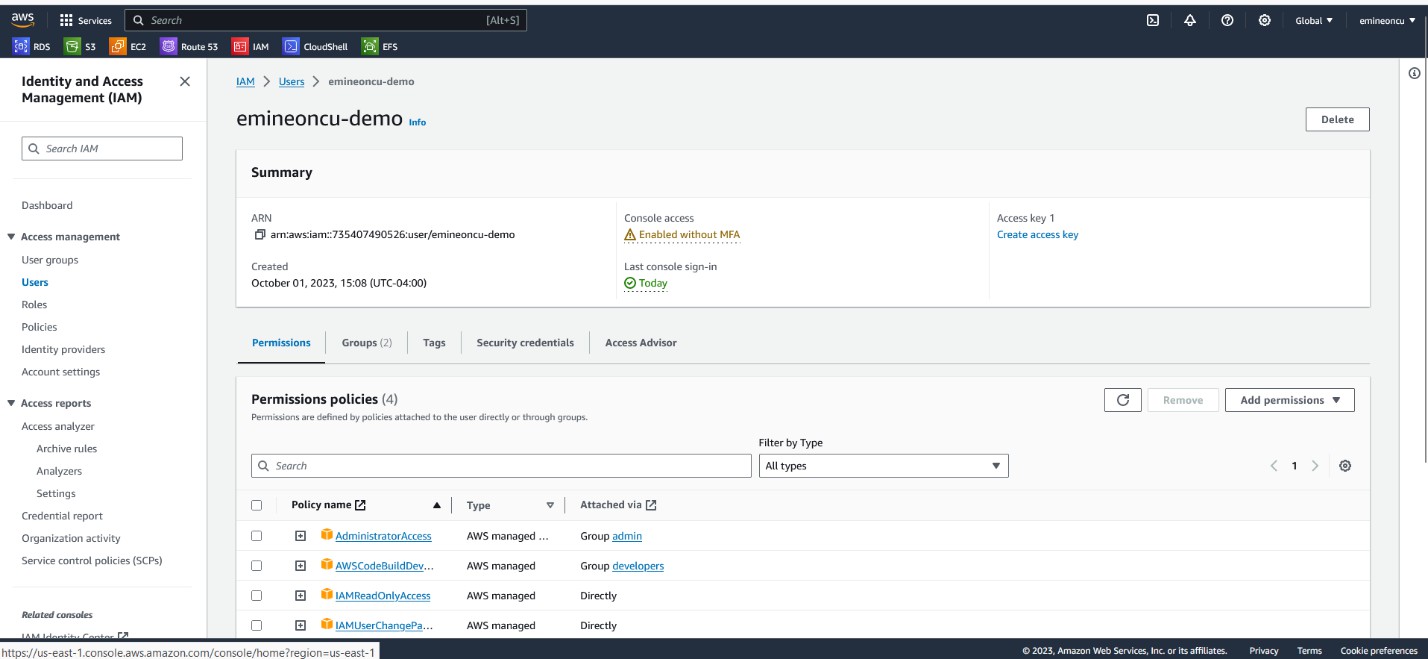
* **We will now be removing the user from the group, and then attaching a policy to the user directly, so the user can access IAM. The screenshot below shows that the user is not able to access IAM because user doesn't have the permissions:**



# Attaching the “IAMReadOnly” permissions to directly to the user



* **Policies can get inherited via groups as well as user being attached directly to a policy:**



* **We now create a role for EC2 instances to be able to access other AWS services. Essential when apps are deployed on EC2 instances, apps can access databases, APIs, Lambda functions, etc.**

